Noname manuscript No.
(will be inserted by the editor)

Realization of 2D convolutional codes of rate $\frac{1}{n}$ by separable Roesser models

Telma Pinho · Raquel Pinto · Paula Rocha

DESIGNS CODES AND CRYPTOGRAPHY Vol. 70 Nº. 1-2 p. 241-250
DOI: 10.1007/s10623-012-9768-1

Received: date / Accepted: date

Abstract In this paper, two-dimensional convolutional codes constituted by sequences in $(\mathbb{F}^n)^{\mathbb{Z}^2}$ where $\mathbb{F}$ is a finite field, are considered. In particular, we restrict to codes with rate $\frac{1}{n}$ and we investigate the problem of minimal dimension for realizations of such codes by separable Roesser models. The encoders which allow to obtain such minimal realizations, called R-minimal encoders, are characterized.

Keywords 2D Convolutional codes, Minimal realizations, Separable Roesser model

The work of the authors was partially supported by *FEDER* founds through *COMPETE*–Operational Programme Factors of Competitiveness ("Programa Operacional Factores de Competitividade") and by Portuguese founds through the *Center for Research and Development in Mathematics and Applications* (University of Aveiro) and the Portuguese Foundation for Science and Technology ("FCT–Fundação para a Ciência e a Tecnologia"), within project PEst-C/MAT/UI4106/2011 with COMPETE number FCOMP-01-0124-FEDER-022690.

Center for Research and Development in Mathematics and Applications,
Department of Mathematics, University of Aveiro
E-mail: telma.pinho@ua.pt
· Center for Research and Development in Mathematics and Applications,
Department of Mathematics, University of Aveiro
Tel.: +351-234372543
Fax: +351-234370066
E-mail: raquel@ua.pt
· Center for Research and Development in Mathematics and Applications and
Department of Electrical and Computer Engineering
Faculty of Engineering, University of Oporto
E-mail: mprocha@fe.up.pt

1 Introduction

For the purpose of encoding, two-dimensional data (like images) is usually transformed into 1D sequences and 1D convolutional codes are used. However, this technique does not take advantage of the correlation of data in the two directions. Two-dimensional (2D) convolutional codes are a generalization of one-dimensional (1D) convolutional codes. They were introduced by [6, 22] and generalized to n dimensions (multidimensional convolutional codes) by [7, 23]. However, they were not very developed on the subsequent years. Recently, these codes have been a matter of interest by several authors [2, 3, 14, 15, 24].

In 1D convolutional codes, state-space representations commonly used in systems theory, are very useful for the analysis and construction of these codes. Minimality of these representations is an important subject not only to obtain more efficient implementations with less amount of memory, but also because these representations have useful characteristics for the construction of good codes [9, 19, 20]. These state-space representations are obtained via realizations of the encoders of the code. However, not all the encoders have realizations of minimal dimension. Encoders with such minimal realizations are called minimal encoders and have been an important subject of research in the coding community.

When considering 2D processes, there exist several state-space models [1, 4, 18]. While in the 1D case there exists a characterization of minimality for realization via state-space models, the same does not happen in the 2D case. However, the state-space models introduced by Roesser [18] admit a class of models, called separable, for which this characterization exists. In this paper we consider 2D convolutional codes of rate $\frac{1}{n}$ and characterize the encoders of the code which have minimal dimension when realized by separable Roesser models. A preliminary version of these results was presented in [16], where the results were obtained for a particular class of encoders, although not made explicit in the statement of the main theorem. In this paper we present the general case.

2 Two-dimensional convolutional codes

In this paper we consider two-dimensional (2D) convolutional codes constituted by sequences indexed on $\mathbb{Z}^2$ and taking values in $\mathbb{F}^n$, where $\mathbb{F}$ is a finite field. Such sequences $\{\mathbf{w}(i,j)\}_{(i,j)\in\mathbb{Z}^2}$ can be represented by formal power series

$$\hat{\mathbf{w}}(z_1, z_2) = \sum_{(i,j)\in\mathbb{Z}^2} \mathbf{w}(i,j) z_1^i z_2^j.$$

The set of formal power series over $\mathbb{F}^n$ is denoted by $\mathcal{F}_\infty^n$, which is a module over the ring of the Laurent polynomials in two indeterminates (2D Laurent polynomials). We denote the ring of 2D Laurent polynomials over $\mathbb{F}$ by $\mathbb{F}[z_1, z_2, z_1^{-1}, z_2^{-1}]$ and the ring of 2D polynomials over $\mathbb{F}$ by $\mathbb{F}[z_1, z_2]$.

Definition 1 [6] A 2D convolutional code $\mathcal{C}$ is a submodule of $\mathcal{F}_\infty^n$ which admits a 2D Laurent polynomial set of generators, i. e., there exist $k \in \mathbb{N}$ and $G(z_1, z_2) \in \mathbb{F}[z_1, z_2, z_1^{-1}, z_2^{-1}]^{n\times k}$ such that

$$\mathcal{C} = \operatorname{Im} G(z_1, z_2) = \{\hat{\mathbf{w}}(z_1, z_2) = G(z_1, z_2)\hat{\mathbf{u}}(z_1, z_2),\ \hat{\mathbf{u}}(z_1, z_2) \in \mathcal{F}_\infty^k\}.$$

In the context of the behavioral approach to systems theory, a 2D convolutional code can be regarded as a linear, shift-invariant, complete controllable behavior [17].

Given a 2D convolutional code $\mathcal{C}$, there always exist a full column rank matrix $G(z_1, z_2) \in \mathbb{F}[z_1, z_2, z_1^{-1}, z_2^{-1}]^{n\times k}$ such that $\mathcal{C} = \operatorname{Im} G(z_1, z_2)$. Such matrix is called an encoder of $\mathcal{C}$. Two encoders, $G_1(z_1, z_2) \in \mathbb{F}[z_1, z_2, z_1^{-1}, z_2^{-1}]^{n\times k_1}$ and $G_2(z_1, z_2) \in \mathbb{F}[z_1, z_2, z_1^{-1}, z_2^{-1}]^{n\times k_2}$ are said to be equivalent if they generate the same code $\mathcal{C}$. In this case, there exist two full row rank matrices over $\mathbb{F}[z_1, z_2, z_1^{-1}, z_2^{-1}]$, $P_1(z_1, z_2)$ and $P_2(z_1, z_2)$ such that

$$G_1(z_1, z_2)P_1(z_1, z_2) = G_2(z_1, z_2)P_2(z_1, z_2).$$

If $G_1(z_1, z_2)$ is right factor prime[1] and $G_2(z_1, z_2)$ is equivalent to $G_1(z_1, z_2)$ then

$$G_2(z_1, z_2) = G_1(z_1, z_2)P(z_1, z_2),$$

for some full row rank Laurent polynomial matrix $P(z_1, z_2)$. In case $G_1(z_1, z_2)$ and $G_2(z_1, z_2)$ are both right factor prime then they have the same number of columns ($k_1 = k_2$) and $G_2(z_1, z_2) = G_1(z_1, z_2)U(z_1, z_2)$, for some unimodular Laurent polynomial matrix $U(z_1, z_2)$ [5,17].

In this paper we focus on 2D convolutional codes of rate $\frac{1}{n}$, which are the ones that admit encoders of size $n \times 1$.

3 Minimal 1D realizations

Given a polynomial matrix $G(z) \in \mathbb{F}[z]^{n\times k}$, we say that $G(z)$ admits a realization $\Sigma = (A, B, C, D)$ of dimension m, through equations of the form

$$\begin{cases} x(t+1) = Ax(t) + Bu(t) \\ w(t) = Cx(t) + Du(t), \end{cases} \tag{1}$$

where $A \in \mathbb{F}^{m\times m}$, $B \in \mathbb{F}^{m\times k}$, $C \in \mathbb{F}^{n\times m}$ and $D \in \mathbb{F}^{n\times k}$, if $G(z) = D + C(I_m - Az)^{-1}Bz$. This means that starting from zero initial conditions, $x(0) = 0$, and an input sequence $\hat{\mathbf{u}}(z) = \sum_{t\geq 0} \mathbf{u}_t z^t$, the system Σ produces the output sequence $\hat{\mathbf{w}}(z) = \sum_{t\geq 0} \mathbf{w}_t z^t$ given by $\hat{\mathbf{w}}(z) = G(z)\hat{\mathbf{u}}(z)$. A realization of $G(z)$ is said to be minimal if it has minimal dimension among all realizations of $G(z)$.

[1] A polynomial matrix $G(z_1, z_2) \in \mathbb{F}[z_1, z_2]^{n\times k}$ is right factor prime if for every factorization $G(z_1, z_2) = \bar{G}(z_1, z_2)T(z_1, z_2)$, with $\bar{G}(z_1, z_2) \in \mathbb{F}[z_1, z_2]^{n\times k}$ and $T(z_1, z_2) \in \mathbb{F}[z_1, z_2]^{k\times k}$, $T(z_1, z_2)$ is invertible in $\mathbb{F}[z_1, z_2]^{k\times k}$.

There exist several algorithms in the literature to obtain minimal realizations of a polynomial matrix [5,10]. The minimal dimension of a realization Σ of a polynomial matrix $G(z)$ is called the McMillan degree of $G(z)$ and is represented by $\mu(G)$.

In order to characterize the McMillan degree of a polynomial matrix let us consider the following definition.

Definition 2 Let $G(z) \in \mathbb{F}[z]^{n\times k}$, $n \geq k$, with column degrees $\nu_1, \nu_2, \ldots, \nu_k$.

The internal degree of $G(z)$, intdeg$G(z)$, is the maximum degree of its full size minors and the external degree of $G(z)$, extdeg$G(z)$, is given by $\sum_{i=1}^{k} \nu_i$.

Moreover, we say that $G(z)$ is column reduced if intdeg$G(z) =$ extdeg$G(z)$.

Proposition 1 *Let $G(z) \in \mathbb{F}[z]^{n\times k}$. If $N(z) \in \mathbb{F}[z]^{n\times k}$ and $D(z) \in \mathbb{F}[z]^{k\times k}$, invertible, are such that $G(z) = N(z)D(z)^{-1}$, with $\begin{bmatrix} N(z) \\ D(z) \end{bmatrix}$ right prime and column reduced, it follows that the McMillan degree of $G(z)$ is given by $\mu(G) =$ extdeg $\begin{bmatrix} N(z) \\ D(z) \end{bmatrix} =$ intdeg $\begin{bmatrix} G(z) \\ I_k \end{bmatrix}$.*

Proof It is well known that the McMillan degree of $G(z)$ is extdeg $\begin{bmatrix} N(z) \\ D(z) \end{bmatrix}$, see for example [5,10].

Since $\begin{bmatrix} G(z) \\ I_k \end{bmatrix}$ and $\begin{bmatrix} N(z) \\ D(z) \end{bmatrix}$ are right prime and $\begin{bmatrix} G(z) \\ I_k \end{bmatrix} D(z) = \begin{bmatrix} N(z) \\ D(z) \end{bmatrix}$, it follows that $D(z)$ is unimodular and hence intdeg $\begin{bmatrix} N(z) \\ D(z) \end{bmatrix} =$ intdeg $\begin{bmatrix} G(z) \\ I_k \end{bmatrix}$. Because $\begin{bmatrix} N(z) \\ D(z) \end{bmatrix}$ is column reduced, we have that extdeg $\begin{bmatrix} N(z) \\ D(z) \end{bmatrix} =$ intdeg $\begin{bmatrix} G(z) \\ I_k \end{bmatrix}$.

Note that from the above proposition it follows that the McMillan degree of a polynomial matrix $G(z)$ is the maximum degree of its minors. Thus, if $G(z)$ is a column matrix its McMillan degree coincides with its column degree.

4 Minimal 2D realizations of 2D encoders

When considering the realization problem of 2D convolutional codes, one can choose among different state-space models for two-dimensional processes [1,4, 18]. However, for some of these models minimality is not easily characterized. We shall consider here a special type of models known as the *separable Roesser models*. In these models the state updating in one of the two directions can be done separately from the other direction [18]. Such models are particulary nice since they admit a necessary and sufficient condition for minimality that can be expressed in terms of the model parameters. Moreover, the dynamics along the direction with separate updating is one-dimensional. In [12] it is shown that all 2D quarter-plane causal rational matrices in z_1 and z_2 with separable denominator can be realized by separable models. The polynomial encoders of a 2D convolutional code are included in this class of matrices. From now on we only consider this type of encoders.

Moreover we consider separable Roesser models $\Sigma = (A_1, A_3, A_4, B_1, B_2, C_1, C_2, D)$ of the form:

$$\begin{cases} x^h(i+1,j) = A_1 x^h(i,j) + B_1 u(i,j) \\ x^v(i,j+1) = A_3 x^h(i,j) + A_4 x^v(i,j) + B_2 u(i,j) \\ w(i,j) = C_1 x^h(i,j) + C_2 x^v(i,j) + D u(i,j), \end{cases} \tag{2}$$

where, for $i, j \geq 0$, $x^h(i,j) \in \mathbb{F}^{m_1}$, $x^v(i,j) \in \mathbb{F}^{m_2}$ and $x(i,j) = \begin{bmatrix} x^h(i,j) \\ x^v(i,j) \end{bmatrix}$ represents the local state, $u(i,j) \in \mathbb{F}^k$ represents the input, $w(i,j) \in \mathbb{F}^n$ the output, A_1, A_3, A_4, B_1, B_2, C_1,C_2 and D are matrices over $\mathbb{F}$ of proper dimensions[2]. The system described by (2) is said to have dimension $m_1 + m_2$. Considering the initial conditions $x(i,0) = x(0,j) = 0$ for all $i, j \geq 1$ and an input $\hat{\mathbf{u}}(z_1, z_2)$, the system Σ produces the output $\hat{\mathbf{w}}(z_1, z_2) = G_\Sigma(z_1, z_2)\hat{\mathbf{u}}(z_1, z_2)$, where

$$G_\Sigma(z_1, z_2) = D + \begin{bmatrix} C_1 \ C_2 \end{bmatrix} \left(\begin{bmatrix} z_1^{-1} I_{m_1} & 0 \\ 0 & z_2^{-1} I_{m_2} \end{bmatrix} - \begin{bmatrix} A_1 & 0 \\ A_3 & A_4 \end{bmatrix} \right)^{-1} \begin{bmatrix} B_1 \\ B_2 \end{bmatrix}.$$

If $G_\Sigma(z_1, z_2) = G(z_1, z_2)$ we say that Σ realizes $G(z_1, z_2)$ and therefore the corresponding 2D convolutional code $\mathcal{C} = \operatorname{Im} G(z_1, z_2)$.

The following theorem gives a procedure for obtaining a minimal realization for a polynomial matrix $G(z_1, z_2) \in \mathbb{F}[z_1, z_2]^{n \times k}$.

Theorem 1 *[13] Let $G(z_1, z_2) \in \mathbb{F}[z_1, z_2]^{n \times k}$. Write*

$$G(z_1, z_2) = G_2(z_2) G_1(z_1) \tag{3}$$

with

$$G_2(z_2) = \left[I_n | I_n z_2 | \cdots | I_n z_2^{\ell_2} \right] N_2, \tag{4}$$

where N_2 is a full column rank constant matrix, and

$$G_1(z_1) = N_1 \begin{bmatrix} I_k \\ I_k z_1 \\ \vdots \\ I_k z_1^{\ell_1} \end{bmatrix} \tag{5}$$

where N_1 is a full row rank constant matrix.

Let $\Sigma_1 = (A_1, B_1, C_1, D_1)$ and $\Sigma_2 = (A_2, B_2, C_2, D_2)$ be 1D minimal realizations of $G_1(z_1)$ and $G_2(z_2)$ of dimension $m_1 = \operatorname{intdeg} \begin{bmatrix} G_1(z_1) \\ I_{\ell_1+1} \end{bmatrix}$ and $m_2 = \operatorname{intdeg} \begin{bmatrix} G_2(z_2) \\ I_{\ell_2+1} \end{bmatrix}$, respectively. Then $\Sigma_{2D} = (\bar{A}_1, \bar{A}_3, \bar{A}_4, \bar{B}_1, \bar{B}_2, \bar{C}_1, \bar{C}_2, \bar{D})$, where

[2] These models have separate updating along the horizontal direction. It is also possible to consider separable Roesser models with separate updating along the vertical direction.

$\bar{A}_1 = A_1,\ \bar{B}_1 = B_1,\ \bar{A}_3 = B_2C_1,\ \bar{A}_4 = A_2,\ \bar{B}_2 = B_2D_1,\ \bar{C}_1 = D_2C_1,\ \bar{C}_2 = C_2$ and $\bar{D} = D_2D_1$, is a 2D minimal realization of $G(z_1, z_2)$ of dimension $m_1 + m_2$.

The factorization of $G(z_1, z_2)$ presented in (3), (4) and (5) in the above theorem, can be easily determined by writing

$$G(z_1, z_2) = \left[I_n | I_n z_2 | \cdots | I_n z_2^{\ell_2}\right] N \begin{bmatrix} I_k \\ I_k z_1 \\ \vdots \\ I_k z_1^{\ell_1} \end{bmatrix},$$

where N is a constant matrix. If N has rank p, there exists a full column rank constant matrix N_2 with p columns, and a full row rank constant matrix N_1 with p rows such that $N = N_2N_1$.

Example 1 Consider

$$G(z_1, z_2) = \begin{bmatrix} 1 + z_1^2 + z_1z_2 + z_2z_1^2 \\ 1 + 2z_1 + 3z_1^2 + 2z_1^2z_2 + z_1z_2 + z_2 \end{bmatrix} = \begin{bmatrix} 1 & 0 & z_2 & 0 \\ 0 & 1 & 0 & z_2 \end{bmatrix} \begin{bmatrix} 1 & 0 & 1 \\ 1 & 2 & 3 \\ 0 & 1 & 1 \\ 1 & 1 & 2 \end{bmatrix} \begin{bmatrix} 1 \\ z_1 \\ z_1^2 \end{bmatrix}.$$

Since $\begin{bmatrix} 1 & 0 & 1 \\ 1 & 2 & 3 \\ 0 & 1 & 1 \\ 1 & 1 & 2 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 1 & 2 \\ 0 & 1 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix}$ with $N_2 = \begin{bmatrix} 1 & 0 \\ 1 & 2 \\ 0 & 1 \\ 1 & 1 \end{bmatrix}$ full column rank and $N_1 = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix}$ full row rank, let us consider $G(z_1, z_2) = G_2(z_2)G_1(z_1)$ with $G_2(z_2) = \begin{bmatrix} 1 & 0 & z_2 & 0 \\ 0 & 1 & 0 & z_2 \end{bmatrix} N_2$ and $G_1(z_1) = N_1 \begin{bmatrix} 1 \\ z_1 \\ z_1^2 \end{bmatrix}$. $\Sigma_2 = \left(\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 1 & 2 \end{bmatrix} \right)$ and $\Sigma_1 = \left(\begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}, \begin{bmatrix} 1 \\ 0 \end{bmatrix} \right)$ are minimal 1-D realizations of $G_2(z_2) = \begin{bmatrix} 1 & z_2 \\ 1 + z_2 & 2 + z_2 \end{bmatrix}$ and $G_1(z_1) = \begin{bmatrix} 1 + z_1^2 \\ z_1 + z_1^2 \end{bmatrix}$, respectively, with dimensions 2 (obtained by applying the realization algorithm presented in (Section 5, [5])). Thus

$$\Sigma = \left(\begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 2 & 3 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \end{bmatrix} \right),$$

obtained by applying Theorem 1, is a minimal realization of $G(z_1, z_2)$ of dimension 4.

5 Minimal 2D realizations of 2D convolutional codes of rate $\frac{1}{n}$

Given a polynomial matrix $G(z_1, z_2)$ we define the *Roesser McMillan degree* of $G(z_1, z_2)$, $\mu_R(G)$, as the minimal dimension of a realization as in (2) of $G(z_1, z_2)$. Different polynomial encoders of a 2D convolutional code may have different Roesser McMillan degrees. Given a 2D convolutional code $\mathcal{C}$, we define the *Roesser McMillan degree* of $\mathcal{C}$, $\mu^*(\mathcal{C})$, as the minimum of the Roesser McMillan degrees of all the polynomial encoders of $\mathcal{C}$. The polynomial encoders with Roesser McMillan degree equal to $\mu^*(\mathcal{C})$ are called *Roesser minimal* (R-minimal) encoders of $\mathcal{C}$.

The aim of this section is to characterize the R-minimal encoders of a 2D convolutional code of rate $\frac{1}{n}$. In the 1D case, the minimal encoders of a convolutional code of rate $\frac{1}{n}$ are the right prime encoders. Here we show that this also holds in the 2D case.

Theorem 2 *Let $\mathcal{C}$ be a 2D convolutional code of rate $\frac{1}{n}$. Then the R-minimal encoders of $\mathcal{C}$ are the right factor prime encoders of $\mathcal{C}$.*

Proof First observe that two right factor prime encoders of $\mathcal{C}$, $G(z_1, z_2)$ and $\bar{G}(z_1, z_2)$ differ by a nonzero constant and thus minimal 2D realizations as in (2) of $G(z_1, z_2)$ and $\bar{G}(z_1, z_2)$ have the same dimension.

Now, let us consider an encoder $G(z_1, z_2)$ of $\mathcal{C}$ and an equivalent encoder $\tilde{G}(z_1, z_2) = G(z_1, z_2)p(z_1, z_2)$ for some polynomial $p(z_1, z_2) \in \mathbb{F}[z_1, z_2]$ and let us see that $\mu_R(\tilde{G}) \geq \mu_R(G)$.

Write $p(z_1, z_2) = p_0(z_2) + p_1(z_2)z_1 + \cdots + p_{k_1}(z_2)z_1^{k_1}$, where $p_i(z_2) \in \mathbb{F}[z_2]$, $i = 0, \ldots, k_1$ with $p_{k_1}(z_2) \neq 0$, and $G(z_1, z_2) = G_2(z_2)G_1(z_1)$, with $G_2(z_2) = [I_n \,|\, I_n z_2 \,|\cdots|\, I_n z_2^{\ell_2}]N$, where N is a constant matrix and $G_1(z_1) = \begin{bmatrix}1 \cdots z_1^{\ell_1}\end{bmatrix}^T$ for some $\ell_1, \ell_2 \in \mathbb{N}$. Let us consider two cases.

<u>Case 1</u>: N is full column rank. Write $G_2(z_2) = \begin{bmatrix}C_0(z_2) \cdots C_{\ell_1}(z_2)\end{bmatrix}$, where $C_i(z_2) \in \mathbb{F}[z_2]^n$, $i = 0, \ldots, \ell_1$, are the columns of $G_2(z_2)$. Then

$$\begin{aligned} G(z_1, z_2)p(z_1, z_2) &= \begin{bmatrix}C_0(z_2)\ C_1(z_2) \cdots C_{\ell_1}(z_2)\end{bmatrix} \begin{bmatrix}1 \\ \vdots \\ z_1^{\ell_1}\end{bmatrix} p(z_1, z_2) \\ &= \begin{bmatrix}C_0(z_2)\ C_1(z_2) \cdots C_{\ell_1}(z_2)\end{bmatrix} P(z_2) \begin{bmatrix}1 \\ z_1 \\ \vdots \\ z_1^{k_1+\ell_1}\end{bmatrix}, \end{aligned}$$

where $P(z_2) = \begin{bmatrix} p_0(z_2) & p_1(z_2) & & p_{k_1}(z_2) & & & 0 \\ & p_0(z_2) & p_1(z_2) & & p_{k_1}(z_2) & & \\ & & \ddots & \ddots & & \ddots & \\ 0 & & & p_0(z_2) & p_1(z_2) & & p_{k_1}(z_2) \end{bmatrix}$

has dimension $(\ell_1 + 1) \times (\ell_1 + k_1 + 1)$. Write

$$G(z_1, z_2)p(z_1, z_2) = \bar{G}_2(z_2)\bar{G}_1(z_1),$$

where $\bar{G}_2(z_2) = \left[C_0(z_2)\; C_1(z_2) \cdots C_{\ell_1}(z_2)\right] P(z_2)$ and $\bar{G}_1(z_1) = \begin{bmatrix} 1 \\ z_1 \\ \vdots \\ z_1^{k_1+\ell_1} \end{bmatrix}$.

Let us see now that there exists a minor of $\bar{G}_2(z_2)$ with degree greater or equal than intdeg $\begin{bmatrix} G_2(z_2) \\ I \end{bmatrix}$. Consider $i_1 < i_2 < \cdots < i_s$ and $j_1 < j_2 < \cdots < j_s$ nonnegative integers. We say that $(i_1, i_2, ..., i_s) < (j_1, j_2, ..., j_s)$ if there exists $r \in \{1, ..., s\}$ such that $i_r < j_r$ and $i_\alpha = j_\alpha$, for $\alpha = 1, ..., r-1$. Let $r_1 < r_2 < \cdots < r_s$ and $t_1 < t_2 < \cdots < t_s$, for some $s \leq 1 + \ell_1$, such that the submatrix of $G_2(z_2)$ constituted by the rows $r_1, r_2, \ldots, r_s$ and the columns $t_1, t_2, \ldots, t_s$ has determinant of degree intdeg$\begin{bmatrix} G_2(z_2) \\ I \end{bmatrix}$ and any other minor constituted by the same rows and by columns $\tilde{t}_1, \tilde{t}_2, \ldots, \tilde{t}_s$ with $(\tilde{t}_1, \tilde{t}_2, \ldots, \tilde{t}_s) < (t_1, t_2, \ldots, t_s)$, has lower degree than the previous one. Let $\bar{j}$ be such that $deg\ p_{\bar{j}}(z_2) = max\{deg\ p_j(z_2) : j = 0, ..., k_1\}$ and $deg\ p_j(z_2) < deg\ p_{\bar{j}}(z_2)$, for $j < \bar{j}$.

Consider now the matrix $M(z_2)$ constituted by the rows $r_1, r_2, \ldots, r_s$ and by the columns $t_1 + \bar{j}, t_2 + \bar{j}, \ldots, t_s + \bar{j}$ of $\bar{G}_2(z_2)$. Since the column i of $\bar{G}_2(z_2)$ is equal to $\displaystyle\sum_{\{f,g \in \mathbb{N}: f \leq \ell_1, g \leq k_1, f+g = i-1\}} C_f(z_2) p_g(z_2)$, for $i = 1, \ldots, \ell_1 + k_1 + 1$, det $M(z)$ can be written as a sum of minors of the form

$$\prod_{i=1}^{s} p_{y_i}(z_2) \det \left[\tilde{C}_{t_1+\bar{j}-1-y_1}(z_2)\; \tilde{C}_{t_2+\bar{j}-1-y_2}(z_2) \cdots \tilde{C}_{t_s+\bar{j}-1-y_s}(z_2)\right], \tag{6}$$

where $y_i \in \{0, ..., k_1\}$ and $\tilde{C}_{t_1+\bar{j}-1-y_i}(z_2)$ is the submatrix of $C_{t_1+\bar{j}-1-y_i}(z_2)$ constituted by the rows $r_1, r_2, \ldots, r_s$, if $0 \leq t_i + \bar{j} - 1 - y_i \leq \ell_1$, and $\tilde{C}_{t_1+\bar{j}-1-y_i}(z_2) = 0$ otherwise. Note that, for $i = 1, \ldots, s$, if $0 \leq t_i + \bar{j} - 1 - y_i \leq \ell_1$,

$$\det \left[\tilde{C}_{t_1+\bar{j}-1-y_0}(z_2)\; \tilde{C}_{t_2+\bar{j}-1-y_1}(z_2) \cdots \tilde{C}_{t_s+\bar{j}-1-y_s}(z_2)\right]$$

can be a minor (or the symmetric of a minor) of $G_2(z_2)$, or zero, if it has two identical columns. Moreover,

$$p_{\bar{j}}(z_2)^s \det \left[\tilde{C}_{t_1-1}(z_2)\; \tilde{C}_{t_2-1}(z_2) \cdots \tilde{C}_{t_s-1}(z_2)\right] \tag{7}$$

is one of such minors and since deg $p_{\bar{j}}(z_2)^s \geq$ deg $p_{y_1}(z_2) p_{y_2}(z_2) \cdots p_{y_s}(z_2))$ for any $y_i \in \{0, ..., k_1\}$ and the degree of $\det \left[\tilde{C}_{t_1-1}(z_2)\; \tilde{C}_{t_2-1}(z_2) \cdots \tilde{C}_{t_s-1}(z_2)\right]$ is equal to intdeg $\begin{bmatrix} G_2(z_2) \\ I \end{bmatrix}$, (7) has maximum degree among all minors of the form (6). We show now that (7) has greater degree than the other minors of the form (6). For that we divide these minors in two different classes:

1) (6) is such that there exists $i \in \{1, \ldots, s\}$ such that $y_i < \bar{j}$. In this case, $deg\ p_{y_i}(z_2) < deg\ p_{\bar{j}}(z_2)$, and therefore the degree of (6) is smaller than the degree of (7).

2) (6) is such that $y_i \geq \bar{j}$ for all $i \in \{1, \ldots, s\}$ and there exists $\bar{i} \in \{1, \ldots, s\}$ such that $y_{\bar{i}} > \bar{j}$ and $y_i = \bar{j}$ for $i < \bar{i}$. In this case, $t_i + \bar{j} - 1 - y_i = t_i - 1$, for $i < \bar{i}$ and $t_{\bar{i}} + \bar{j} - 1 - y_{\bar{i}} < t_{\bar{i}} - 1$ which means that

$$(t_1 + \bar{j} - 1 - y_1, \ldots, t_{\bar{i}} + \bar{j} - 1 - y_{\bar{i}}, \ldots, t_s + \bar{j} - 1 - y_s) < (t_1 - 1, \ldots, t_s - 1)$$

and therefore

$$\deg \det \begin{bmatrix} C_{t_1+\bar{j}-1-y_1}(z_2) & \cdots & C_{t_s+\bar{j}-1-y_s}(z_2) \end{bmatrix} < \deg \det \begin{bmatrix} C_{t_1-1}(z_2) & \cdots & C_{t_s-1}(z_2) \end{bmatrix}$$

and consequently (6) has degree smaller than (7). Thus $\deg \det M(z_2) \geq \operatorname{intdeg} \begin{bmatrix} G_2(z_2) \\ I \end{bmatrix}$.

To see that $\mu_R(G(z_1, z_2)p(z_1, z_2)) \geq \mu_R(G(z_1, z_2))$ let us factorize

$$G(z_1, z_2)p(z_1, z_2) = \hat{G}_2(z_2)\hat{G}_1(z_1)$$

as in Theorem 1 in such a way that $M(z_2)$ is a submatrix of $\hat{G}_2(z_2)$. Write $\bar{G}_2(z_2) = [I_n \,|\, I_n z_2 \,|\, \cdots \,|I_n z_2^{k_2+\ell_2}]\bar{N}$. Note that since the $t_1 + \bar{j}, t_2 + \bar{j}, \ldots, t_s + \bar{j}$ columns of $\bar{G}_2(z_2)$ are linearly independent over $\mathbb{F}[z_1, z_2]$ then also the $t_1 + \bar{j}, t_2 + \bar{j}, \ldots, t_s + \bar{j}$ columns of $\bar{N}$ are linearly independent over $\mathbb{F}$, which means that there exists a full column rank constant matrix $\hat{N}_2$ which has the $t_1 + \bar{j}, t_2 + \bar{j}, \ldots, t_s + \bar{j}$ columns of $\bar{N}$ as a submatrix and a full row rank constant matrix $\hat{N}_1$ such that $\bar{N} = \hat{N}_2\hat{N}_1$. Thus $G(z_1, z_2)p(z_1, z_2) = \hat{G}_2(z_2)\hat{G}_1(z_1)$ where $\hat{G}_2(z_2) = [I \,|\, I z_2 \,|\, \cdots \,|I z_2^{k_2+\ell_2}]\hat{N}_2$ and $\hat{G}_1(z_1) = \hat{N}_1 \begin{bmatrix} 1 & z_1 & \cdots & z_1^{k_1+\ell_1} \end{bmatrix}^T$ are such that $\mu_R(G(z_1, z_2)p(z_1, z_2)) = \operatorname{intdeg} \begin{bmatrix} \hat{G}_2(z_2) \\ I \end{bmatrix} + \operatorname{intdeg} \hat{G}_1(z_1)$ and $M(z_2)$ is a submatrix of $\hat{G}_2(z_2)$. Thus, since $\det M(z_2)$ is a minor of $\hat{G}_2(z_2)$ and $\operatorname{intdeg} \hat{G}_1(z_1) = \operatorname{intdeg} G_1(z_1) + k_1$, we have that $\mu_R(G(z_1, z_2)p(z_1, z_2)) \geq \operatorname{intdeg} \begin{bmatrix} G_2(z_2) \\ I_{\ell_1+1} \end{bmatrix} + \operatorname{intdeg} \hat{G}_1(z_1) = \mu_R(G(z_1, z_2))$.

<u>Case 2:</u> N is not full column rank. Then there exists an upper triangular matrix T with $1's$ in the diagonal such that $N = \tilde{N}_2 T$ where $\tilde{N}_2$ is obtained from N by substituting a column i by zero if it is linear combination of the columns $1, \ldots, i-1$. Let $i_1 < i_2 < \cdots < i_p$ be the nonzero columns of $\tilde{N}_2$, where $p = \operatorname{rank} \tilde{N}_2$. Then $N = N_2 N_1$ where N_2 is the full column rank constant matrix constituted by the columns $i_1, i_2, \ldots, i_p$ of $\tilde{N}_2$ and N_1 is the full row rank matrix constituted by the $i_1, i_2, \ldots, i_p$ rows of T. Thus $G(z_1, z_2) = G_2(z_2)G_1(z_1)$ where

$$G_2(z_2) = [I \,|\, I z_2 \,|\, \cdots \,|I z_2^{\ell_2}]N_2 \text{ and}$$

$$G_1(z_1) = \begin{bmatrix} z_1^{i_1-1}(1 + a_1^1 z_1 + a_2^1 z_1^2 + \cdots + a^1_{\ell_1-(i_1-1)} z_1^{\ell_1-(i_1-1)}) \\ z_1^{i_2-1}(1 + a_1^2 z_1 + a_2^2 z_1^2 + \cdots + a^2_{\ell_1-(i_2-1)} z_1^{\ell_1-(i_2-1)}) \\ \vdots \\ z_1^{i_p-1}(1 + a_1^p z_1 + a_2^p z_1^2 + \cdots + a^p_{\ell_1-(i_p-1)} z_1^{\ell_1-(i_p-1)}) \end{bmatrix},$$

for some $a^i_j \in \mathbb{F}$, for $i = 1, \ldots, p$, $j = 1, \ldots, \ell_1-(i_1-1)$. Then $G(z_1, z_2)p(z_1, z_2) = G_2(z_2)P(z_2)\left[1 \cdots z_1^{\ell_1+k_1}\right]^T$, where $P(z_2)$ is a $p \times (\ell_1 + k_1 + 1)$ matrix with the j-th row given by

$$\left[0_{1\times i_j}\ p^j_0(z_2)\ p^j_1(z_2) \cdots p^j_{\ell_1+k_1-i_j}(z_2)\right],$$

where $p^j_r(z_2) = p_r(z_2) + \sum_{s=1}^{r} a^j_s p_{r-s}(z_2)$, considering $p_r(z_2) = 0$ if $r > k_1$, $a^j_s = 0$ if $s > \ell_1 - (j-1)$ and $p_{r-s}(z_2) = 0$ if $r - s > k_1$, for $j = 1, \ldots, p$. Note that if $\bar{j}$ is such that deg $p_{\bar{j}}(z_2) = \max\{\text{deg } p_i(z_2) : i = 0, ..., k_1\}$ and deg $p_i(z_2) <$ deg $p_{\bar{j}}(z_2)$, for $i < \bar{j}$ then deg $p^j_{\bar{j}}(z_2) = \max\{\text{deg } p^j_i(z_2) : i = 0, ..., k_1\}$ and deg $p^j_i(z_2) <$ deg $p^j_{\bar{j}}(z_2)$, for $i < \bar{j}$. Applying a similar reasoning as in Case 1, we conclude that also $\mu_R(G(z_1, z_2)p(z_1, z_2)) \geq \mu_R(G(z_1, z_2))$.

The following corollary follows immediately from the proof of Theorem 2.

Corollary 1 *Let $G(z_1, z_2) \in \mathbb{F}[z_1, z_2]^{n\times 1}$ be an encoder of a 2D convolutional code with a minimal realization of dimension m, and $p(z_1, z_2) \in \mathbb{F}[z_1, z_2]$ such that*

$$p(z_1, z_2) = p^1_0(z_2) + p^1_1(z_2)z_1 + p^1_2(z_2)z_1^2 + \cdots + p^1_{r_1}(z_2)z_1^{r_1},$$

with $p^1_i(z_2) \in \mathbb{F}[z_2]$, $i = 0, \ldots, r_1$ and $p^1_{r_1}(z_2) \neq 0$, for some $r_1 \in \mathbb{N}$. Define $r_2 = \max_{0\leq i\leq r_1}$ deg $p^1_i(z_2)$. Then the minimal dimension of the realizations of $\bar{G}(z_1, z_2) = G(z_1, z_2)p(z_1, z_2)$ is greater or equal than $m + r_1 + r_2$.

Moreover, consider $G(z_1, z_2) = G_2(z_2)G_1(z_1)$ a factorization of $G(z_1, z_2)$ as in Theorem 1. If $G_2(z_2)$ is row reduced, then a minimal realization of $\bar{G}(z_1, z_2)$ has dimension $m + nr_2 + r_1$.

Example 2 Let

$$G(z_1, z_2) = \begin{bmatrix} 1 + z_1^2 + z_1z_2 + z_2z_1^2 \\ 1 + 2z_1 + 3z_1^2 + 2z_1^2z_2 + z_1z_2 + z_2 \end{bmatrix}$$

be the encoder presented in Example 1 which minimal realizations have dimension 4 and consider the equivalent encoder $\bar{G}(z_1, z_2) = G(z_1, z_2)(1 + z_1^2 + z_1z_2)$. Since $G_2(z_2)$ obtained in Example 1 is row reduced, by Corollary 1 we conclude that $\mu_R(\bar{G}(z_1, z_2)) = 8 = 4 + n * r_2 + r_1$, where $r_2 = 1$ and $r_1 = 2$.

6 Conclusions

In this paper we have studied the minimality of realizations of 2D convolutional codes by separable Roesser models. We have showed that, similarly to the 1D case, the R-minimal encoders of a 2D convolutional code of rate $\frac{1}{n}$ are the right factor prime encoders. Minimal realizations have been widely used in 1D convolutional codes, not only for construction of good codes as also for the implementation of efficient decoding algorithms. Since the separable Roesser models can be obtained by two 1D realizations, we think that 1D constructions of good convolutional codes can be used to construct good 2D convolutional codes. The construction of optimal 2D convolutional codes of rate $1/n$ was solved in [2] for a very particular case. The general construction of such codes with optimal distance is still an open problem. Similarly, 1D decoding algorithms can be used to implement decoding algorithms for 2D convolutional codes. As far as we know, there is no decoding algorithm available for 2D convolutional codes.

An interesting although difficult problem is to characterize the R-minimal encoders of a 2D convolutional code of rate $\frac{k}{n}$, with $k > 1$. We believe that the R-minimal encoders will be a proper subset of the right factor prime encoders, as happens in the 1D case.

References

1. S. Attasi, Systmes Lineaires Homogenes a Deux Indices, Rapport Laboria, 31, (1991)
2. J.J. Climent, D. Napp, C. Perea and R. Pinto, A construction of MDS 2D convolutional codes of rate 1/n based on superregular matrices, Linear Algebra and its Applications, 437, 766-780 (2012)
3. C. Charoelarpnopparut, Applications of Gr obner bases to the structural description and realization of multidimensional convolutional code. ScienceAsia, 35:95-105 (2009)
4. E. Fornasini and G. Marchesini, Algebraic Realization Theory of Two-Dimensional Filters, Variable Structure Systems - Lecture Notes in Economics and Mathematical Systems
5. E. Fornasini and R. Pinto, Matrix Fraction Descriptions in Convolutional Coding, Linear Algebra and its Applications, 392, 119-158 (2004)
6. E. Fornasini and M. E. Valcher, Algebraic Aspects of Two-Dimensional Convolutional Codes, IEEE Transactions on Information Theory, 40, 1068-1082 (1994)
7. H. Gluesing-Luerssen, J. Rosenthal and P. A. Weiner, Duality between multidimensional convolutional codes and systems, In F. Colonius, U. Helmke, F. Wirth, and D. Pratzel-Wolters, editors, Advances in Mathematical Systems Theory, A volume in Honor of Diedrich Hinrichsen, 135-150 (2000)
8. T. Hinamoto, Realizations of a State-Space Model from Two- Dimensional Input-Output Map, In Transactions on Circuits and Systems, 27, 36-44 (1980)
9. R. Hutchinson, J. Rosenthal and R. Smarandache, Convolutional codes with maximum distance profile, Systems & Control Letters, 54 (1), 53-63 (2005)
10. T. Kailath, Linear Systems. Prentice Hall, Englewood Cliffs (1980)
11. M.M.S. Kung, B.C. Levy and T. Kailaht, New Results in 2D Systems Theory, Part II: 2D State-Space Models Realization and the Notions of Controllability, Observability, and minimality, IEEE, 65, 945-961 (1977)
12. T. Lin, M. Kawamata, T. Higuchi, Decomposition of 2D Separable- Denominator Systems: Existence, Uniqueness, and Applications, IEEE Trans. on Circuits and Systems, 34, 292-296 (1987)
13. T. Lin, M. Kawamata, T. Higuchi, On Controllability, Observability, and Minimality of 2D Separable-Denominator Systems: A New Approach Based on the Reduced-Dimensional Decomposition, IEEE Trans. on Circuits and Systems, 34, 962-967 (1987)
14. R.G. Lobo, D.L. Bitzer, and M.A. Vouk. Locally invertible multivariate polynomial matrices. In Coding and cryptography, volume 3969 of Lecture Notes in Comput. Sci., 427-441. Springer, Berlin (2006)
15. D. Napp, C. Perea, and R.Pinto. Input-state-output representations and constructions of finite support 2D convolutional codes. Advances in Mathematics of Communications, 4(4):533-545 (2010)
16. T. Pinho, R. Pinto and P. Rocha, Minimal realizations of a 2D convolutional code of rate $1/n$ by separable Roesser models, 3rd International Castle Meeting on Coding Theory and Applications, J. Borges and M. Villanueva, 219-224, Cardona (2011)

17. P. Rocha and J. Willems, Controllability of 2D Systems, IEEE Transactions on Automatic Control,413-423 (1991)
18. R. P. Roesser, A Discrete State-Space Model for Linear Image Processing, IEEE Trans. Autom. Control, 20,1-10 (1975)
19. J. Rosenthal and E. York, BCH convolutional codes, IEEE Transactions on Information Theory, 45(6), 1833-1844 (1999)
20. R. Smarandache and J. Rosenthal, A state space approach for constructing MDS rate 1/n convolutional codes, In: 1998 Information Theory Workshop. Piscataway, NJ, 116-117 (1998)
21. A.J. Tether, Construction of Linear State-Variable Models from Finite Input-Output Data, IEEE Trans. Autom. Control, 15, 427-436 (1970)
22. M.E. Valcher and E. Fornasini, On 2D finite support convolutional codes: an algebraic approach, Multidimensional Systems and Signal Processing, 5:231-243 (1994)
23. P. A. Weiner, Multidimensional Convolutional Codes, PhD thesis, Department of Mathematics, University of Notre Dame, Indiana, USA, April (1998)
24. E. Zerz, On multidimensional convolutional codes and controllability properties of multidimensional systems over finite rings, Asian Journal of Control, 12(2): 119-126 (2010)